IN THE UNITED STATES DISTRICT COURT FOR THE WESTERN DISTRICT OF MISSOURI SOUTHERN DIVISION

JOSHUA GLASSCOCK, on behalf of himself and all others similarly situated,	)	
	)	
Plaintiff,	)	
	)	
v.	)	Case No. 22-CV-3095-SRB
	)	
SIG SAUER, INC.,	)	
	)	
Defendant.	)	

ORDER GOVERNING FORMAT FOR DOCUMENT PRODUCTIONS

WHEREAS, counsel for Plaintiff and Defendants (collectively, the "Parties," and each, a "Party") have met and conferred regarding discovery of electronically stored information ("ESI") of the Parties;

WHEREAS, the Parties have reached agreement on certain of the issues discussed regarding such discovery;

WHEREAS, the Parties have entered into this Stipulated Format for Document Productions ("Protocol") to facilitate the just, speedy, and inexpensive conduct of discovery involving electronically stored information ("ESI") and to promote, to the fullest extent possible, the resolution of disputes regarding the discovery of ESI and document production without Court intervention;

1. General Stipulations

   a. The Parties have entered into this Stipulated Format for Document Productions ("Protocol") to facilitate the just, speedy, and inexpensive conduct of discovery involving paper documents and ESI through reasonable, precise, and cost-effective strategies regarding the discovery of ESI and document production

without Court intervention.

b. Paper documents and ESI should be produced in accordance with the Federal Rules of Civil Procedure. The proportionality standard set forth in Fed. R. Civ. P. 26(b)(1) shall be applied in all matters related to discovery of ESI, including without limitation the preservation, collection, and production of such information. The Parties recognize and take into consideration the unique ability of each Party to evaluate its own ESI and determine the appropriate procedures, methodologies, and technologies for preserving, collection, and production of documents.

c. The procedures and protocols outlined herein govern the production of all documents and ESI, including all computer generated information or data of any kind, by the Parties. This Protocol governs all Parties to these proceedings, whether they are currently involved or become so in the future. All disclosures and productions made pursuant to this Protocol are subject to the Stipulated Protective Order entered in this matter.

2. Production Format Protocols

a. Except as provided in Section 4 or elsewhere in this Order, all production images will be produced as single page Group IV Tagged Image File Format (.TIF or .TIFF) files at 300 x 300 dpi resolution and 8.5 x 11 inch page size, unless a document requires a higher resolution in order to be appropriately viewed.

b. Documents or ESI containing color need not be produced initially in color and may be produced in black and white. If an original color image is produced in black and white, the receiving Party may for good cause request the producing

Party to produce the image in color. Following a request for color production, the Parties will meet and confer on a reasonable, cost effective means of providing the requested document in color. The default for color images will be TIFF format or as single page JPEG format.

c. A unique Bates number shall be assigned to each page, and branded in the lower right-hand corner of the page, but shall not obscure any part of the underlying image. All Bates numbering will be sequential within a given document and use a consistent font and size throughout the production with no special characters or embedded spaces included in the Bates.

d. Any confidentiality or other endorsements shall be branded on the lower left-hand corner of the page. The Parties shall use reasonable measures to ensure that any such branding does not obscure any part of the underlying image. No additional branding or designation made in reference to the document request to which a document may be responsive is required.

e. A searchable, document-level text file shall be provided for each paper document or ESI file produced as TIFF images. Each such file will have a filename matching the Bates number applied to the first page of the corresponding static image file or placeholder file, followed by the .TXT extension. For ESI, the Parties agree that the searchable, document-level text file shall be created directly from the native file. For ESI from which text cannot be extracted, for redacted documents, or for paper documents, the Parties agree that they will produce document-level OCR text for each such document. To the extent practicable, the Parties will consider producing searchable text in ANSI format.

f. **Load/Unitization File:** The Parties agree that the producing Party will provide the following load files for all productions:

- **Metadata Import File**: DAT format, in ASCII format (e.g., .txt, .dat, or .csv), using Concordance default delimiters to separate the fields and records.
- **Image Cross-Reference File**: Standard Opticon delimited file in .OPT format, containing the corresponding image information and indicating page breaks.

g. Only one Metadata Import File and (if appropriate) one Image Cross-Reference File should be included with each production. The Metadata Import File should contain the metadata fields detailed and described in Exhibit A and/or Exhibit B of this Protocol, as appropriate. To the extent possible, the Parties agree to populate the CUSTODIAN field for all produced ESI and paper documents, if known and reasonable.

h. Production Media: The Parties agree that documents shall be produced preferably through a secure File Transfer Protocol ("FTP") provided via email or otherwise on physical media ("Physical Media") sent by a method no slower than overnight delivery via USPS, UPS, or FedEx. Acceptable Physical Media includes external hard drives or other electronic media agreed to by the Parties. Each piece of Physical Media shall identify a production number corresponding to the production volume, as well as the volume of the material in that production. Each piece of Physical Media shall also identify: (1) the matter name and case number' (2) the Producing Party's name; (3) the production date; and (4) the

Bates number range of the materials contained on the Physical Media. In the event that a party utilizes an FTP for the production of documents, the information identified in this section to be provided with Physical Media shall be provided in a written production letter ("Transmittal Letter") with the accompanying email providing instructions for accessing documents through the FTP.

i. **Language:** A hard-copy document or ESI that contains a natural language other than English, in whole or in part, shall be produced in the original language. A producing Party is under no obligation to prepare, provide or search for English translations of non-English language documents or ESI.

3. Electronic Production of Paper Documents as Static Images

The Parties agree that to the extent that the producing Party elects to produce hard copy documents in electronic format, such documents will be produced as Single page Group IV Tagged Image File Format (.TIF or .TIFF) files as described above. Additionally:

a. In scanning paper documents, distinct documents should not be merged into a single record, and single documents should be merged into multiple records (*i.e.*, paper documents should be logically unitized). The Parties will use reasonable efforts to have their vendors unitize documents correctly and will commit to address situations where there are improperly unitized documents.

b. The Parties agree that any file folders and/or documents affixed to hard copy documents will be scanned as separate documents.

c. The Parties agree to provide appropriate load/unitization files in accordance with attached Exhibit A and consistent with the specifications for such files set forth

in Section 2, above.

d. The Parties agree that the producing Party also produce searchable optical character recognition ("OCR") text of scanned paper documents consistent with the specifications for Searchable Text set forth in Section 2, above.

4. Production of ESI in Native File Format

The Parties agree that ESI shall be produced as TIFFs with accompanying load file except that certain documents will be produced in native format, specifically:

- Spreadsheet formatted document files (e.g., Microsoft Excel Files)
- Multimedia audio or visual files such as voice and video recordings (e.g., .wav and .mpeg)

The Parties may discuss additional production in native format on a document by document or category by category basis. Any documents produced in native format should be produced in accordance with the following specifications:

a. A unique document number shall be used as the file name, and the original file name and file extension shall be preserved in the corresponding load file.

b. For each produced native file, the producing Party will provide a static image slipsheet indicating that the document was produced in native format and providing the unique Bates number and confidentiality designation for the corresponding native file. Any confidentiality designation will also be provided in the corresponding load file.

c. Prior to a trial or other proceeding at which the receiving party may use a native document, the receiving party agrees to advise the producing party if the native document has been produced without a corresponding TIFF image file.

d. If a document that otherwise would be produced in native format requires redaction, such documents may be produced in TIFF format in accordance with this Protocol.

e. For each document produced in native format, the producing Party will provide all metadata contained in the field identified in Exhibit B.

5. Production of ESI as Static Images

Except for those documents produced in native format pursuant to Section 4, above, the Parties agree that ESI will be produced in TIFF format with accompanying load file as describe in Section 2, above. Additionally:

a. The Parties agree to meet and confer regarding file types that are not amenable to conversion into TIFF images and which may not be easily produced in native file format. If necessary, any such relevant and responsive, but non-convertible files, may be temporarily produced in the form of a placeholder TIFF image.

b. When processing ESI, the Parties agree to use Coordinated Universal Time (UTC) as the time zone.

c. When processing ESI for production as a static image, the Parties agree that "Auto Date" be forced off, and "hidden columns or rows", "hidden worksheets", "speaker notes", "track changes", "comments" and other similar information viewable in the native file be forced on such that the information is preserved to the extent practical and appears on the produced image file.

d. Parent-Child Relationships (i.e., the association between an attachment and its parent conveying document) that have been maintained in the ordinary course of business shall be preserved at processing and production, such that the

attachments appear in order behind the conveying email. A non-responsive attachment within an otherwise produced family shall be represented in the production by a single page slipsheet indicating the attachment is non-responsive and appearing in order behind the conveying responsive email.

e. The Parties are not obligated to manually populate any fields in Appendix B that cannot be extracted from the document using automated processes with the exception of Custodian, BegBates, and EndBates.

f. Known software files identified in the National Software Reference Library database maintained by the National Institute of Standards and Technology ("NIST") need not be collected or produced.

g. In order to reduce the burden of collecting and producing irrelevant and non-substantive material, the Parties are not obligated to collect or produce contact files.

h. To the extent that the Parties request information from enterprise or relational databases or other structured data (e.g. Oracle, SQL Server, DB2), responsive information contained within a database may be produced by querying the database and generating a flat file report or exportable electronic file (e.g., .CSV) of such data along with relevant fields for review by requesting Party.

i. Embedded Objects in an ESI file are to be extracted at processing. Some file types may contain embedded objects, typically found in the following productivity types: MS Excel, MS Word, MS PowerPoint, MS Project, MS Outlook, MS Access, as well as Adobe Acrobat (PDF). Objects within those identified file types shall be extracted as separate files and shall be produced as attachments to

the file in which they were embedded if the file in which these objects are embedded is produced.

j. Documents that are associated by hyperlink or otherwise linked to another location or file without being embedded will not be treated as attached files and will not be produced as if attachments in order behind the document in which they were referenced by link. Such documents will be treated in accordance with their originating location and collected, processed, and produced as governed by the relevant procedures and protocols as outlined in this order for each document's file type and data source.

k. Compressed file types (i.e., .CAB, .GZ, .TAR. .Z, .ZIP) shall be decompressed in a reiterative manner to ensure the compressed file within a compressed file is decompressed into the lowest possible compressing resulting in individual files.

l. The Producing Party will take reasonable steps to unencrypt any discoverable ESI that exists in encrypted format (e.g., password-protected) and that can be reasonably unencrypted based on industry standards for production.

6. Format of Prior-Production Format of Documents

a. Documents produced for litigation or other court proceeding outside of this Litigation may be produced to the Requesting Party in this Litigation in the production format from the prior production. The Receiving Party may thereafter request a meet and confer regarding the form, content or adequacy of any such production including this provision.

7. Redactions

Parties agree that ESI and paper documents may need to be redacted. To the extent that

a responsive document contains non-responsive information unrelated to this matter, information that is protected from disclosure by applicable privilege or immunity, information that is commercially sensitive or proprietary, information that is governed by applicable privacy law or regulation, such as private or personally identifying information, or other information that the Protective Order entered allows to be redacted, the producing Party may produce that document in redacted form. Each page of the document from which information is redacted shall bear a designation that it has been redacted, or when the document has been redacted in full, a single page slipsheet may be produced to provide designation indicating the reason it was withheld from an otherwise produced family. Any confidentiality designation will also be provided in the corresponding load file.

To the extent that any document contains information that is redacted, those documents shall be produced in the form of a redacted .TIFF image. Documents otherwise produced natively, such as Spreadsheets, may be redacted and produced in native format and the Parties will ensure that the original data in the redacted spreadsheets will be preserved.

8. Search Methodology and Data Reduction

To the extent a producing party wishes to use search terms, technology-assisted review, or other electronic search methodologies to cull documents from review and production, the parties shall meet and confer and attempt in good faith to reach agreement regarding the search methodology.

Any search for potentially relevant documents and ESI shall involve searching for such documents in data sources within which such documents and ESI are likely to be most readily

accessible. Data sources that are not reasonably accessible because of undue burden shall not be considered for search. If data sources are identified that are not readily accessible, the Parties shall meet and confer to discuss the necessity of searching such data sources.

9. Deduplication

The Parties shall make reasonable efforts to deduplicate ESI. Parties may deduplicate stand-alone documents or entire document families vertically within each custodian or horizontally (also referred to as globally) across custodians. ESI will be considered duplicative if it has matching MD5 or SHA-1 hash values. Documents with the same content but different metadata can also be identified through the use of near-duplication technology, provided that only documents identified by such technology are 100% near-duplicates shall be considered duplicates for purposes of this paragraph.

When comparing document families, if a parent document is an exact duplicate but one or more attachments or embedded files are not exact duplicates, neither the attachments or embedded files, nor the parent document, will be deduplicated.

Attachments to emails shall not be eliminated from their parent emails by deduplication. Where a responsive stand-alone document is an exact duplicate of an email attachment, the email attachment must be produced and the stand alone document may be deduplicated.

A list of all custodians who were in possession of the document, including those whose copy of the document was removed during deduplication, should be placed in the CUSTODIAN_DUPLICATE (or "DUPLICATE_CUSTODIAN") field, with each entry separated by a semi-colon (;) character, as set forth in Exhibit B.

10. Email Threading and Privileged Documents

In order to reduce the volume of entirely duplicative content within email threads, the

Parties may utilize threading or "email thread suppression." As used in this Protocol, email thread suppression means employing commercially acceptable methods to reduce production of duplicative email threads by producing only the inclusive email messages and their attachments from each email thread. An email message is inclusive when it contains any non-duplicative content or has a document or set of documents attached that does not appear elsewhere within the email thread. Typically, an inclusive email will be either the longest, most recent in time email message containing all of the text from previous, earlier in time email messages within that same thread or an email message with attachments not otherwise attached to a later in time email within that same thread, but any email will be treated as inclusive when it contains non-duplicative content. Accordingly, exact duplicates of emails as well as email messages comprised of text identical to text contained within an inclusive email in the same conversation will be suppressed and not produced, however responsive, non-duplicative attachments will be produced along with their conveying email message even when the text of that parent email message is fully represented in a longer, later in time email thread.

For all responsive documents withheld in their entirety for Privilege, the producing party will produce a Privilege Log explaining the documents withheld. It will be produced within 60 days of the parties' completion of its production. Parties have no obligation to produce or log information generated after the data of the commencement of this litigation.

Duplicative emails suppressed under Section 10 need not be reflected on the Party's privilege log. When there is a chain of privileged emails, the Producing Party need only include one entry on the privilege log for the entire email chain, and need not log each email message contained in the chain separately. In this circumstance, redacted documents from the chain need not be logged as long as (a) for emails, the bibliographic information is not redacted and (b) for

non-email documents, the redaction is noted on the TIFF image.

11. Preservation of ESI

Each Party shall be responsible for taking reasonable and proportional steps to preserve potentially relevant documents and ESI within its possession, custody, or control.

The Parties are not required to modify or suspend, on a going forward basis, the procedures used by them in the ordinary course of business to backup data and systems for disaster recovery and similar purposes related to continuity of operations. The Parties have not taken, and are not required to take, any such backup media out of ordinary rotation.

Pursuant to this Protocol, the Parties have no obligation to preserve, collect or produce the following information or data sources if they are not kept in the ordinary course of business:

a. "Deleted," "slack," "fragmented," or "unallocated" data on hard drives;

b. Random access memory (RAM) or other ephemeral data;

c. Online access data such as temporary internet files, history, cache, cookies, etc.;

d. Data in metadata fields that are frequently updated automatically, such as the "Date Accessed" value in Microsoft Windows operating systems;

e. Known junk files from the NIST list or unimportant data files;

f. Network, server, or software application logs;

g. Structural files not material to individual document contents (e.g. .CSS, .XSL, .XML, .DTD, etc.);

h. System files and files not actively saved by user; and

i. Automated emails not generated by a human author, including but not limited to automated out of office replies.

12. Non-Waiver of Privilege or Protection

Any Party's production of privileged or work-product protected documents, ESI or information shall not constitute a waiver of the privilege or protection with respect to (a) those documents; (b) any other communications or document relating to the subject matter of those documents; or (c) any other communications or documents relating to the individuals or entities who sent, received or are named in those documents in this case or any other federal or state proceeding. These protections apply irrespective of the degree of care taken by the Producing Party in (1) preventing disclosure, it being expressly recognized that the Producing Party is not obligated to engage in any pre-production review of the documents to identify Privileged Materials; or (2) rectifying disclosure, it being further recognized that the Producing Party shall have no obligation to engage in post-production review to determine whether it has produced any Privileged Materials. The Parties reserve the right to challenge any assertion by the Producing Party of attorney-client privilege or work product protection with respect to any particular document or collection/compilation of documents or data. Nothing in this Protocol shall require a Party to produce documents that are protected from disclosure. This paragraph shall be interpreted to provide the greatest protection allowed by law.

The Parties further agree that if a Party receiving information or documents independently determines that the Producing Party produced information that reasonably appears to be subject to a claim of privilege or of protection as trial-preparation material, the Receiving Party shall notify the Producing Party or Parties of the apparent inadvertent disclosure, and (a) must promptly return, sequester, or destroy the specified information and any copies it has; (b) must not use or disclose the information until the claim is resolved; (c) must take reasonable steps to retrieve the information if the Party disclosed it before making the independent determination that the document was privileged; and (d) may promptly present the information to the court under seal

for a determination of the claim. Nothing contained herein is intended to or shall serve to limit a Party's right to conduct a review of documents, ESI or information (including metadata) for relevance, responsiveness and/or segregation of privileged and/or protected information before production.

13. Data Security, Control and Protection

The Parties agree that a Party receiving documents, ESI or other information exchanged in this matter shall take precautions to secure the materials received and prevent unauthorized access, disclosure or dissemination. Parties shall exercise at least the same standard of due and proper care with respect to the storage, custody, use, and/or dissemination of information exchanged in this matter as is exercised by the recipient with respect to its own information of the same or comparable confidentiality and sensitivity. Receiving Parties must take reasonable precautions to protect Confidential or Highly Confidential material from loss, misuse and unauthorized access, disclosure, alteration and destruction, including but not limited to:

a. Confidential or Highly Confidential materials shall be stored and maintained in a reasonably secure manner so as to avoid unauthorized disclosure, including reasonable administrative, technical, and physical safeguards designed to protect the security and confidentiality of such information against unauthorized access and other reasonably anticipated threats or hazards, and that ensures that access is limited to the persons authorized under this Order and the Protective Order.

b. Confidential or Highly Confidential Material in electronic form shall be maintained in a secure litigation support site and/or other electronic sources that apply standard industry practices regarding data security, including but not limited to, application of access control rights to those persons entitled to access the

information under this Order and the Protective Order;

c. A list of current and former authorized users of the Receiving Party's litigation support site shall be maintained while this litigation, including any appeals, is pending;

d. Any Confidential or Highly Confidential Information downloaded from the litigation support site in electronic format shall be stored only on devices (e.g., laptop, tablet, smartphone, USB drive) that are password protected and/or encrypted with access limited to persons entitled to access confidential material under this Order and the Protective Order. If the user is unable to password protect and/or encrypt the device, then the Confidential or Highly Confidential material shall be password protected and/or encrypted at the file level;

e. Confidential or Highly Confidential Information in paper format is to be maintained in the Receiving Party's counsel's law offices or comparably secure location, with access limited to persons entitled to access Protected Information under this Order and the Protective Order; and

f. In the event a Party who received Confidential or Highly Confidential Information experiences a data breach or reasonably believes a breach may have occurred, the Receiving Party shall immediately notify the Producing Party of same, describe the incident and the Confidential or Highly Confidential Information accessed without authorization and cooperate with the Producing Party to address and remedy the breach, as well as to preclude further breaches and to address publicity regarding the breach. The Receiving Party shall take such actions as are required by applicable laws, including privacy laws. After notification, the Receiving Party

shall keep the Designating Party informed of remediation efforts. Nothing herein shall preclude the Producing Party from asserting legal claims or constitute a waiver of legal rights and defenses in the event of litigation arising out of the Receiving Party's failure to appropriately protect Confidential or Highly Confidential Information from unauthorized disclosure.

14. Limitation

Nothing in this Protocol shall be interpreted to require disclosure of irrelevant information or relevant information protected by the attorney-client privilege, work-product doctrine, or any other applicable privilege or immunity.

This Protocol does not address, limit, or determine the authenticity, admissibility, relevance, discoverability, or agreement to produce of any document or ESI. The Parties are not waiving the right to seek any discovery and are not waiving any objections to any discovery requests.

All documents produced hereunder are fully protected and covered by the Parties' confidentiality agreements, by any clawback agreements entered into by the Parties, and by the Stipulated Protective Order and any other applicable orders entered by this Court in this matter. If the Producing Party is producing a Document subject to a claim that it is protected from disclosure under the Stipulated Protective Order, the Producing Party shall make the designation as described in the Stipulated Protective Order.

IT IS SO ORDERED.

/s/ Stephen R. Bough
STEPHEN R. BOUGH, JUDGE
UNITED STATES DISTRICT COURT

DATE: October 11, 2022

EXHIBIT A

Fields for Production of Paper Documents Converted to Static Images

Note: The chart below describes the fields to be produced with the Load / Unitization Files in generic, commonly used terms. Field names may vary from the below.

Field	Definition
CUSTODIAN	Name of person from whose files the document is produced
BEGBATES	Beginning Bates Number (production number)
ENDBATES	End Bates Number (production number)
BEGATTACH	First Bates number of family range (i.e., Bates number of the first page)
ENDATTACH	Last Bates number of family range (i.e., Bates number of the last page of the last attachment)
PGCOUNT	Number of pages in the document
TEXTPATH	File path for OCR or Extracted Text files

EXHIBIT B

Fields for Production of ESI

Note: The chart below describes the fields to be produced with the Load / Unitization Files in generic, commonly used terms. Field names may vary slightly from the below.

Field	Doc	Definition
CUSTODIAN	All	Name of person or non-custodial datasource from whose files the document is produced
DUPLICATE_CUSTODIAN or CUSTODIAN_DUPLICATE	All	Custodian, plus any additional Custodian(s) who had a duplicate copy removed during global deduplication (with each Custodian separated by a semicolon (;) character)
BEGBATES	All	Beginning Bates Number (production number)
ENDBATES	All	End Bates Number (production number)
BEGATTACH	All	First Bates number of family range (i.e., Bates number of the first page)
ENDATTACH	All	Last Bates number of family range (i.e., Bates number of the last page of the last attachment)
PGCOUNT	All	Number of pages in the document
FILETYPE/APPLICATION	All	Application used to create document
FILEEXT	All	File extension of the native file (e.g., XLS, DOC, PDF)
FILEPATH	eDocs	File source path for all electronically collected documents, which includes location, folder name
FILENAME	eDocs	File name of the original electronically collected documents
DOCTYPE	All	Descriptive field created by the vendor processing software (e.g. email, edoc, image, attachment)

HASHVALUE	All	MD5 Hash or SHA Value created during processing
FROM	eMail	Sender of email
TO	eMail	Recipient of email
CC	eMail	Additional Recipients of email
BCC	eMail	Blind Additional Recipients of email
SUBJECT	eMail	Subject line of email
DATESENT (mm/dd/yyyy hh:mm)	eMail	Date and Time Sent
DATERCVD (mm/dd/yyyy hh:mm)	eMail	Date and Time Received
DATECRTD (mm/dd/yyyy hh:mm)	eDoc	Creation Date and Time
LASTMODD (mm/dd/yyyy hh:mm)	eDoc	Last Modified Date and Time
TITLE	eDoc	Title field value extracted from the metadata of the native file.
AUTHOR	eDoc	Creator of a document
LASTAUTHOR	eDoc	Last Saved By field contained in the metadata of the native file
CONFIDENTIALITY	eDoc	Confidentiality designation for documents produced in native format
NATIVEFILELINK	All	For documents provided in native format
TEXTPATH	All	File path for OCR or Extracted Text files